IHRE MITARBEITER IM FOKUS DER HACKER – SCHUTZ DURCH KÜNSTLICHE INTELLIGENZ

PETER ROSENDAHL // 04.05.2022

AGENDA

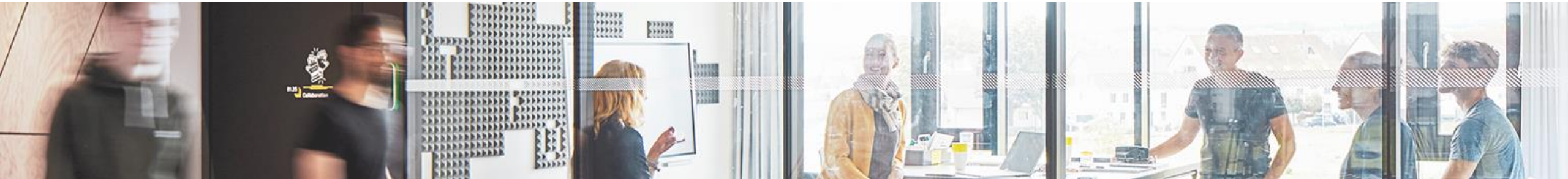
1
Prävention, Detektion und Reaktion

2
Weiterentwicklung der IAM Strategie

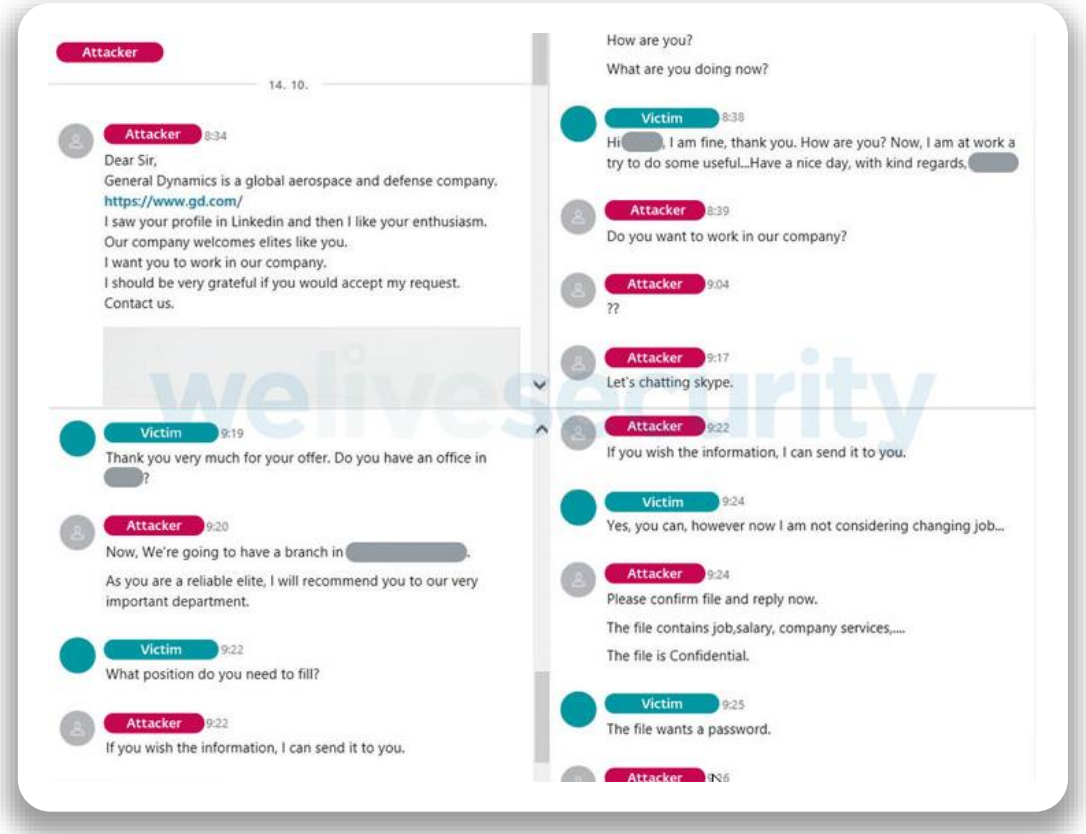
3
Gefahren erkennen und richtig reagieren!

4
Wie Sie starten sollten

1 PRÄVENTION, DETEKTION UND REAKTION



PHISHING FUNKTIONIERT (FAST) IMMER



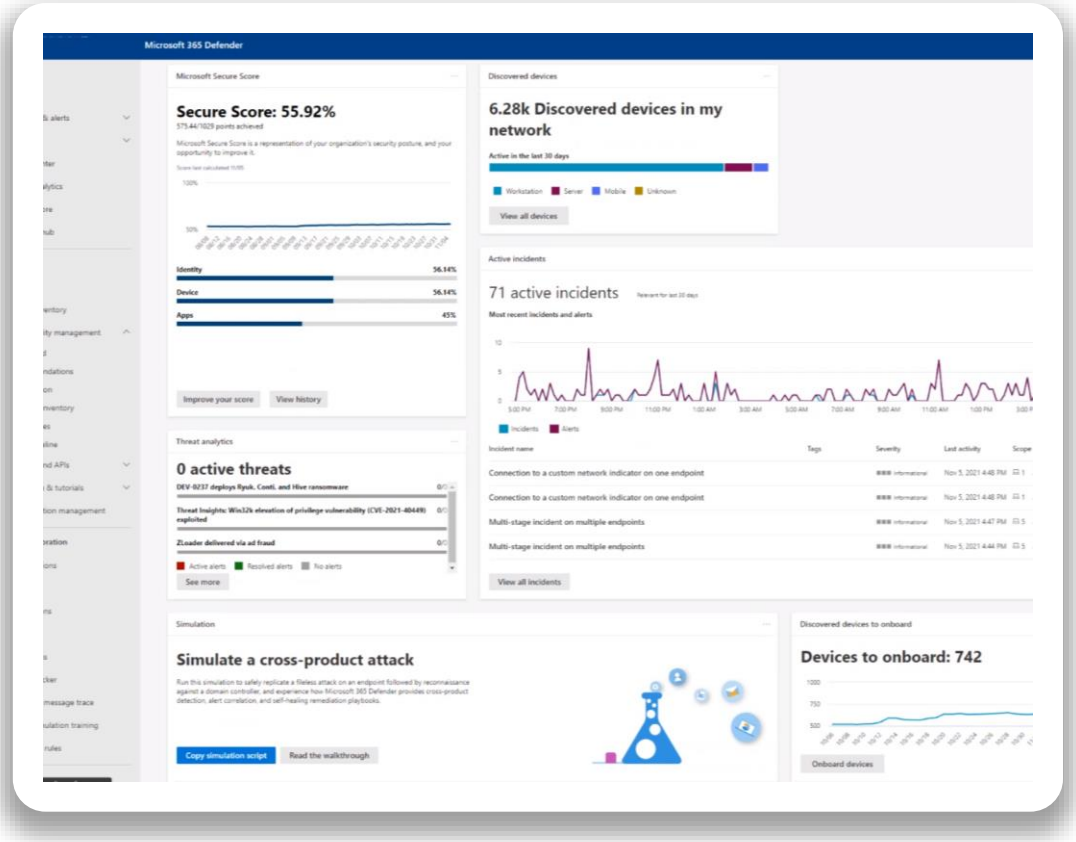
Quelle: Hackers Target Military and Aerospace Staff by Posing as HRs Offering Jobs (thehackernews.com)

WORAN ERKENNT MAN EINEN HACKER?

WOHER WEIß ICH, DASS ICH EIN OPFER WURDE?

WAS PASSIERT, WENN ICH ES MERKE?

HACKERANGRIFFE IN IHREM UNTERNEHMEN SIND NICHT LEICHT ZU ERKENNEN



HÄTTEN SIE DAS BEMERKT?

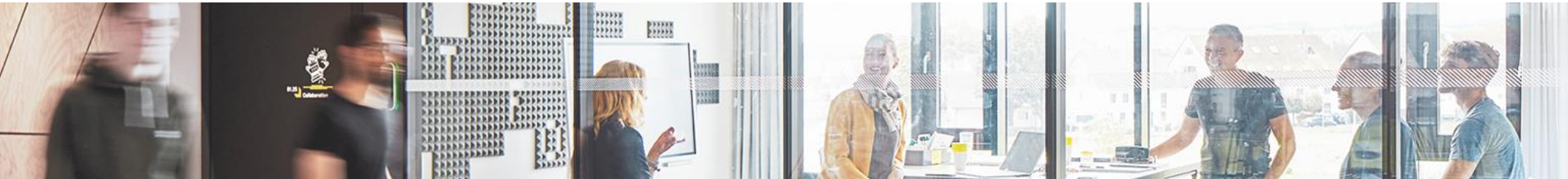
HÄTTEN SIE DAS GEWUSST?

WIE HÄTTEN „SIE“ REAGIERT?

BITTE NUR GUTE NACHRICHTEN

„Ihr Sicherheitsvorfall in der Presse ist keine gute Schlagzeile!“

2 WEITERENTWICKLUNG DER IAM STRATEGIE



IAM ROADMAP

PHASE 1

Das Chaos beherrscht die digitalen Identitäten und ihre Berechtigungen

PHASE 2

Identity & Access Management-Prozesse und ein Basisrollenkonzept sind definiert.

PHASE 3

IAM-Prozesse sind automatisiert.

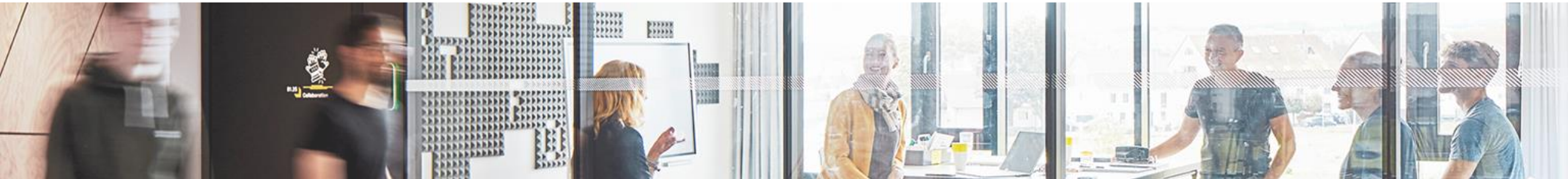
PHASE 4

Identity Governance und User Self Services sind implementiert.

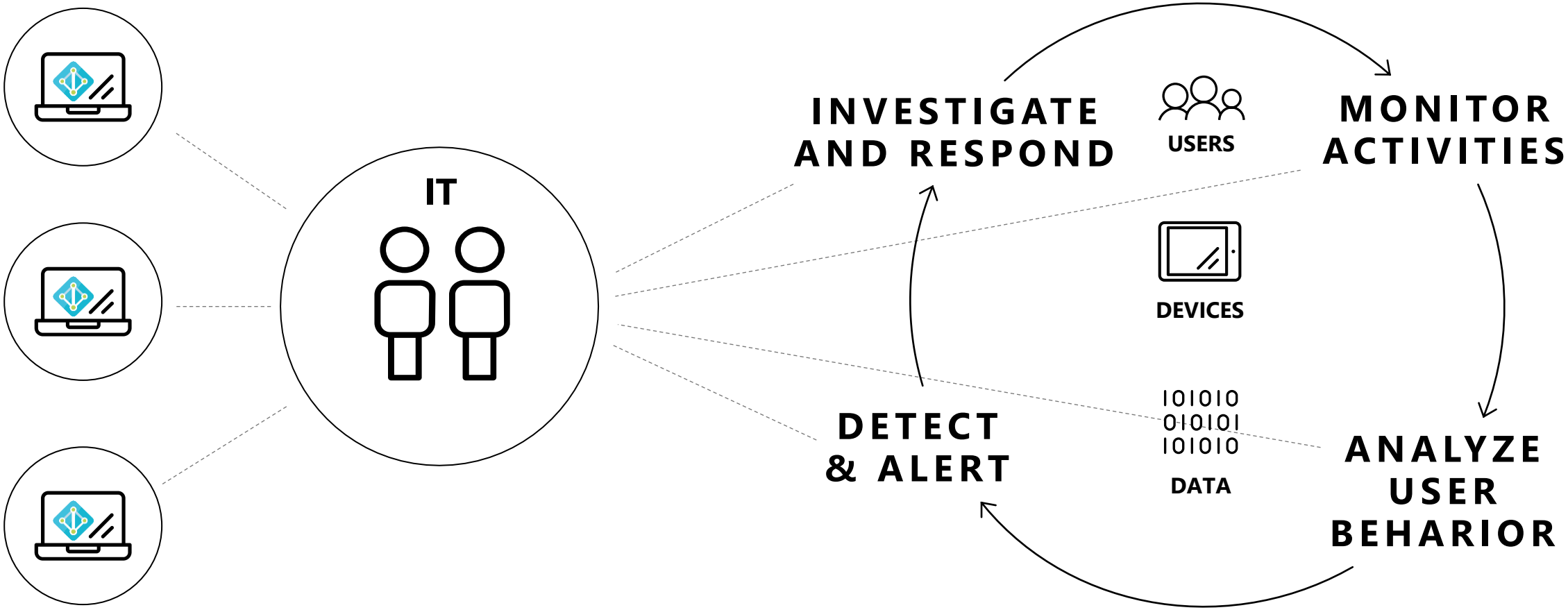
PHASE 5

Erweiterter Schutz der digitalen Identität

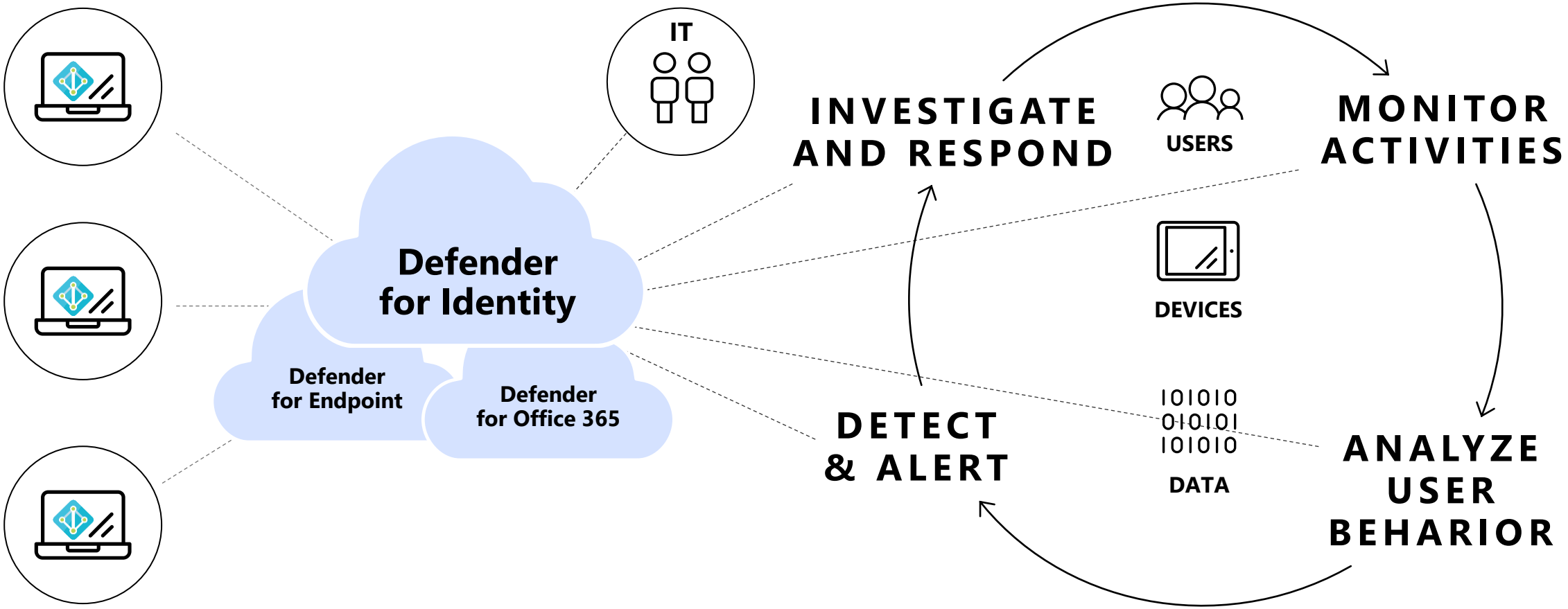
3 GEFAHREN ERKENNEN UND RICHTIG REAGIEREN



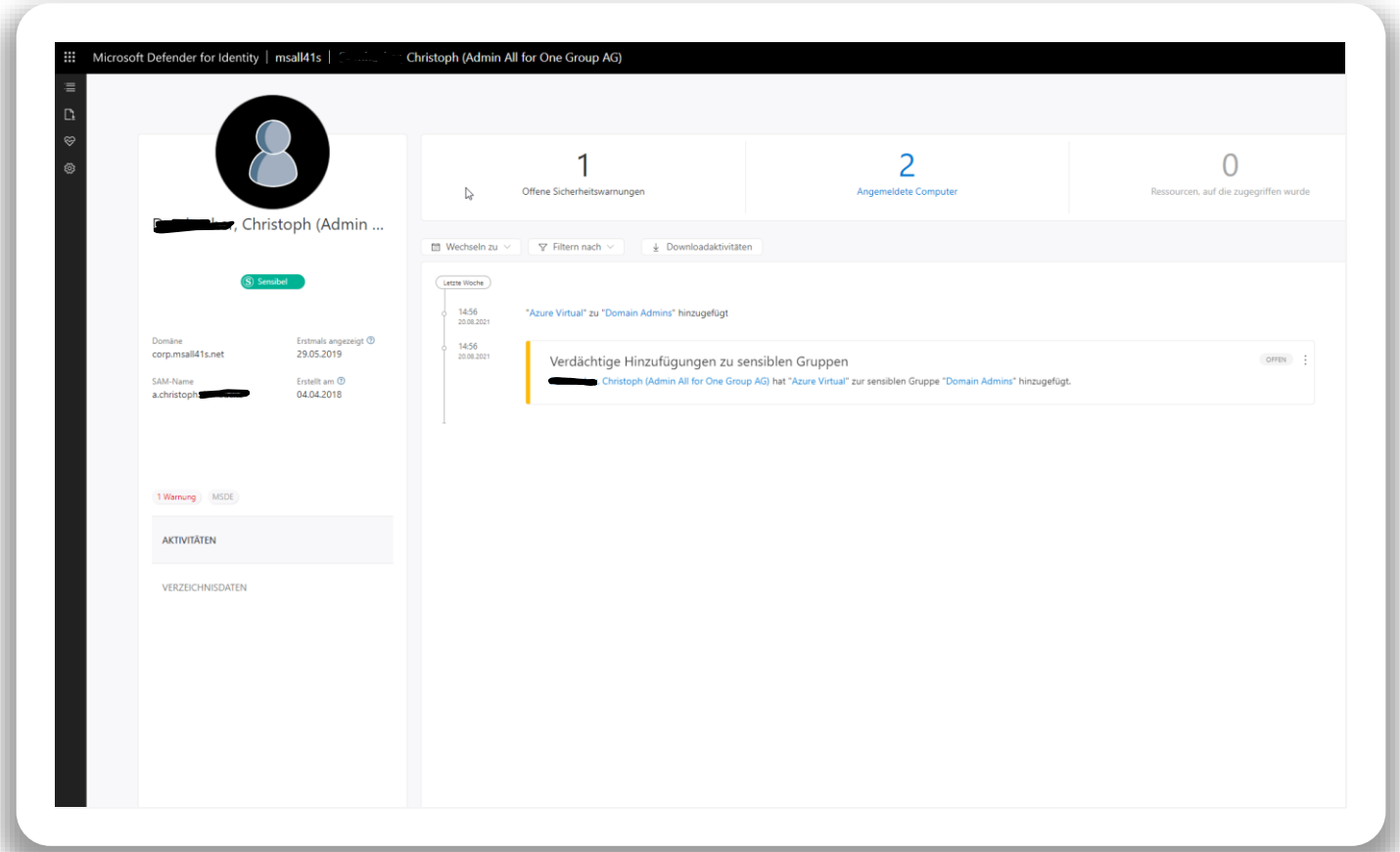
ANGRIFFSERKENNUNG IST EINE HERAUSFORDERUNG!



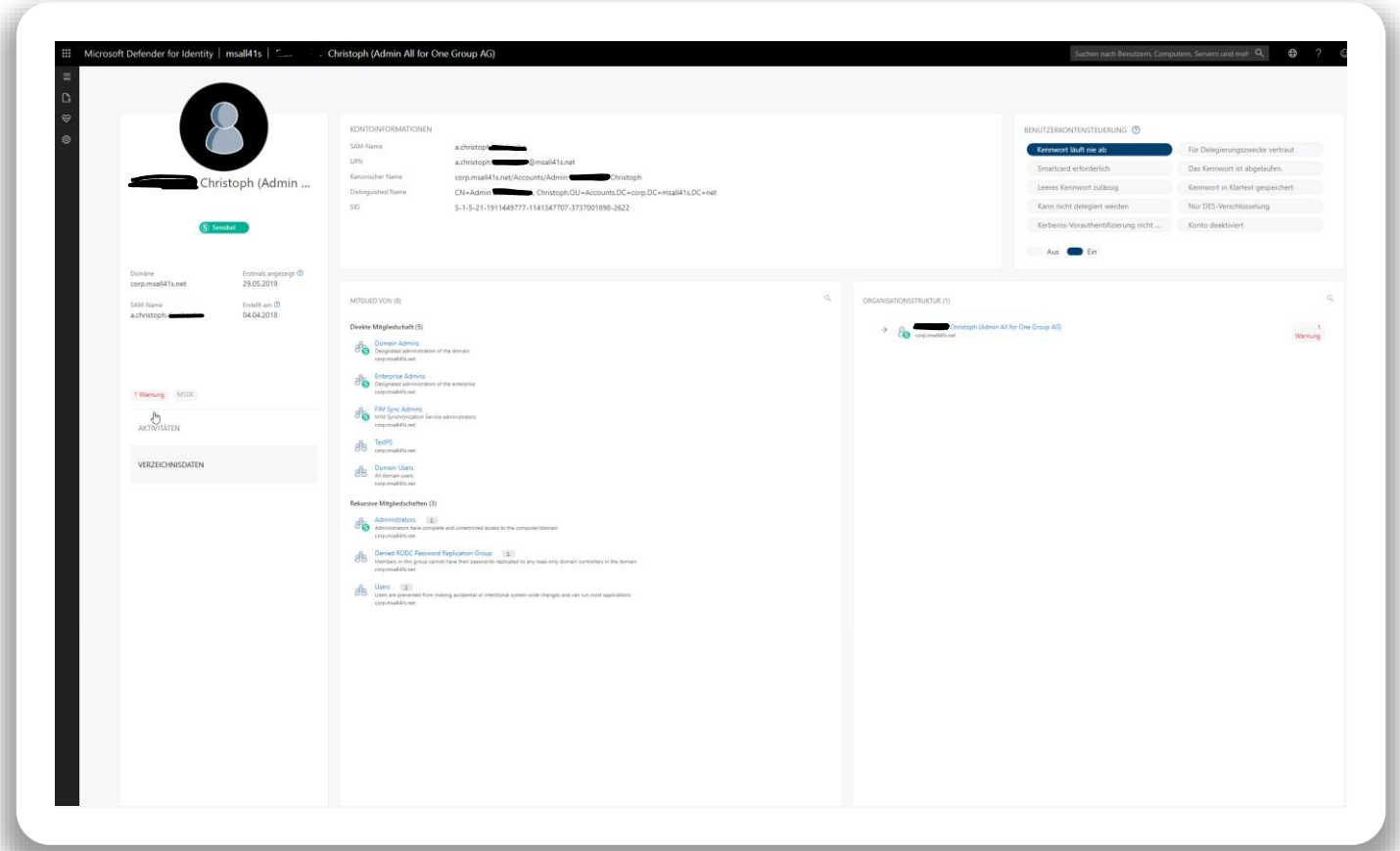
ANGRIFFSERKENNUNG MIT DEFENDER FOR IDENTITY



EIN INTEGRIERTES COCKPIT

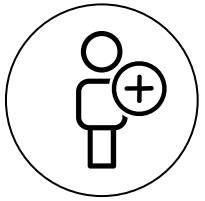


EIN INTEGRIERTES COCKPIT



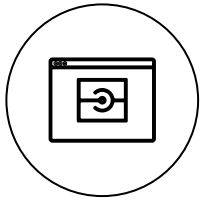
CONDITIONAL ACCESS

Benutzer



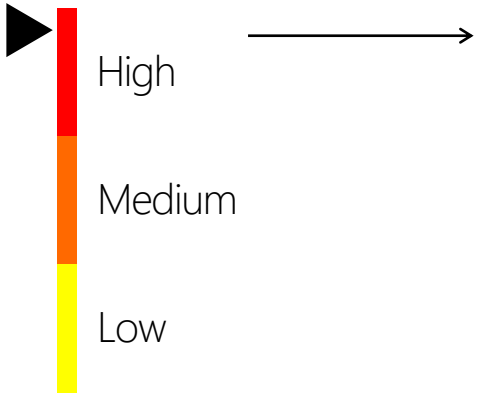
- **Rolle:** Sales
- **Gruppe:** Mitarbeiter Deutschland
- **Device:** Windows
- **Lokation:** Filderstadt, DE
- **Letze Anmeldung:** vor 5 Stunden

Gerät



- **Health:** Gerät konform
- **Client:** Browser konform
- **Config:** Unternehmen
- **Last seen:** Singapore, SG

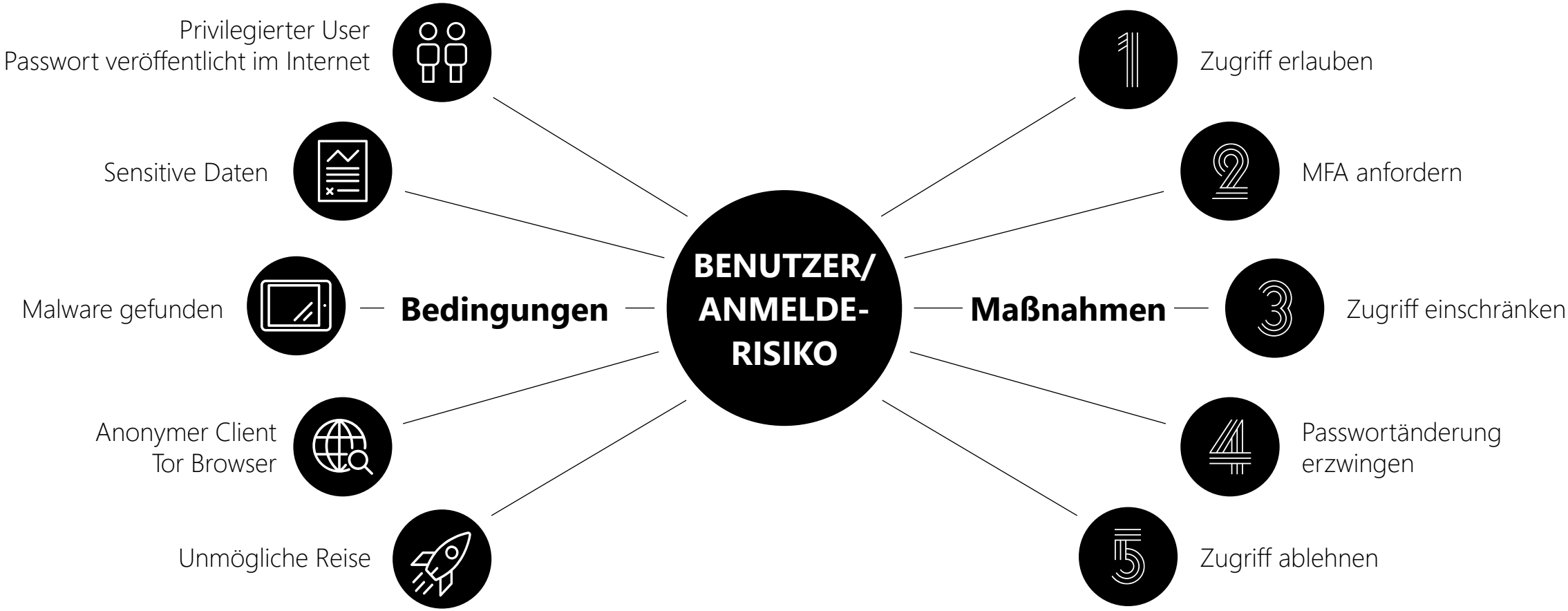
Conditional access risk



Zugriff auf Unternehmens-ressourcen blockieren

Beseitigung der Bedrohung

CLOUD IDENTITY PROTECTION



PRIVILEGED IDENTITY MANAGEMENT

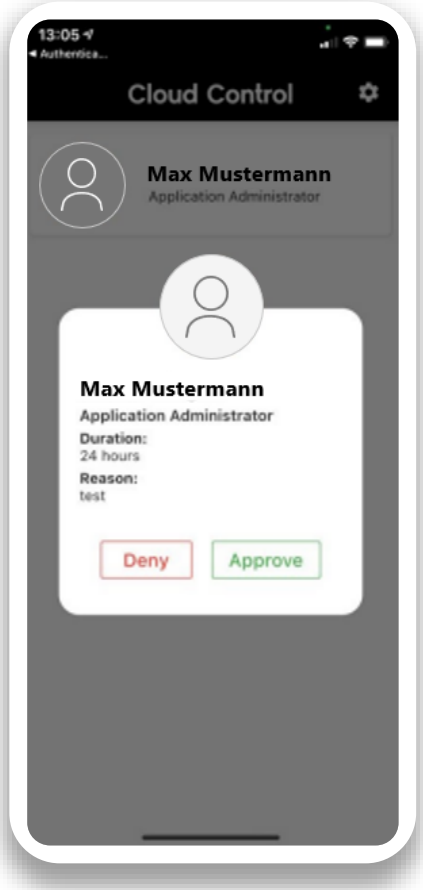
Erkennen, Einschränken und Überwachen von privilegierten Identitäten in der Microsoft Cloud

Durchsetzung von On-Demand- und Just-in-Time-Zugriff

Transparenz durch Warnmeldungen, Auditberichte und Zugriffsprüfungen

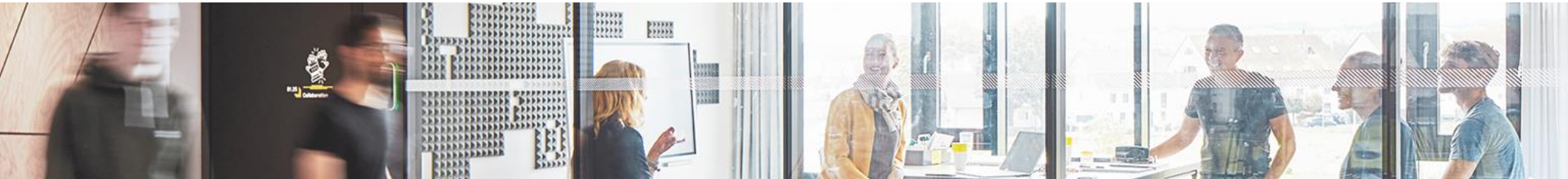
Erzwingung von Multifaktor-Authentifizierung

ZIEL: „ZERO STANDING ACCESS"



SCHNELL UND EINFACH – DIE "PIM APP" DER ALL FOR ONE

4 WIE SIE STARTEN SOLLTEN

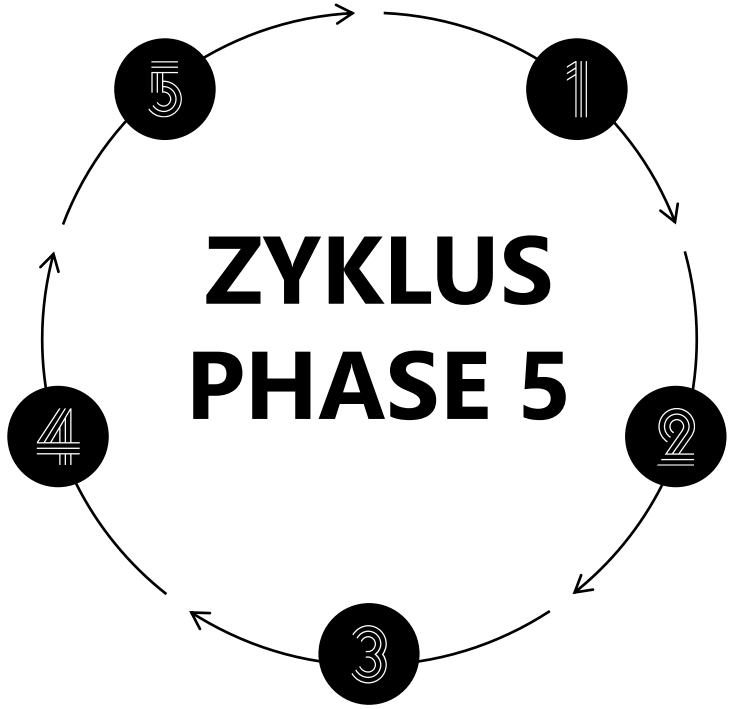


VALIDIERUNG

Monitoring, Penetration Test, Red/Blue Teaming

ANALYSE

Anforderungen, Systemlandschaft und Lizenzen



SERVICE MANAGEMENT

Definition der Prozesse und Integration eines Service Providers

OPTIMIERUNG

Evaluation, Implementierung, Quick-Wins, Lösungskomponenten

AWARENESS UND KNOWHOW

IT und Mitarbeiter

//

Phase 1-4: All for One Identity und Security Workshops

IDENTITY MANAGEMENT PROZESSE – INITIALANALYSE

Inhalt des Angebots

Zentrale Mitarbeiter-Identitätsverwaltung und -pflege: Von On-Boarding über eine Versetzung bis hin zum Off-Boarding – über alle Systeme und Cloud-Plattformen hinweg.

Ihr unmittelbarer Mehrwert

Ein tieferes Verständnis über die Wichtigkeit von Identitäten und deren Verwaltung in einer heterogenen IT-Landschaft und den sich daraus ergebenden Risiken und Bedrohungen sowie ein ausführliches Ergebnisdokument.

Leistungsbestandteile

Ganztägiger Workshop durchgeführt von zwei erfahrenen Security-Architekten als Interview zur Erfassung des Ist-Zustandes und zur Ermittlung relevanter Daten-quellen und Zielsysteme. Ergebnisprä-sentation für alle internen Stakeholder.

Ihr nachhaltiger Nutzen

Optimale standardisierte Grundlage zur Reorganisation dezentraler Identitäten und regelkonforme Überwachung der Gültigkeit von Berechtigungen – für eine erhöhte Sicherheit und Compliance Ihres Unternehmens.

An wen richtet sich dieses Angebot primär?

- Sicherheitsbeauftragte/ CISOs
- IT-Leiter / CIOs
- Personalleiter / CHRO
- Leiter Infrastruktur oder SAP-Systeme

Jetzt Initialanalyse anfragen:

www.all-for-one.com/iam-workshop

Weitere Informationen zu Identity Mgmt: cc.all-for-one.com

IDENTITÄTS- UND PASSWORT-/PHISHING-ANGRIFFE SIND BILLIG!

ENTLASTEN SIE IHRE IT-FACHKRÄFTE!

TAKE AWAYS

ALL FOR ONE HAT FÜR SIE DEN RICHTIGEN EINSTIEG ZUR WEITERENTWICKLUNG DER IAM STRATEGIE!

KONTAKT

PETER ROSENDAHL

DIRECTOR SOLUTIONS
CYBERSECURITY, CLOUD ARCHITECTURE & NEW WORK

T +49 7131394019

M +49 15152642338

Peter.Rosendahl@all-for-one.com

DISCLAIMER

Die Informationen in diesen Unterlagen sind vertraulich und dürfen nicht ohne vorherige schriftliche Genehmigung durch All for One Group SE bekannt gegeben werden. Alle Texte, Bilder und Grafiken unterliegen dem Urheberrecht und anderen Gesetzen zum Schutz des geistigen Eigentums. Alle Rechte an diesen Unterlagen sind der All for One Group SE vorbehalten.
All for One Group SE stellt diese Unterlagen ohne jegliche Verpflichtung, Gewährleistung oder Garantie, weder ausdrücklich noch stillschweigend, zur Verfügung. All for One Group SE übernimmt keine Verantwortung für Fehler oder Irrtümer in diesem Dokument, es sei denn, derartige Schäden beruhen auf Vorsatz oder grober Fahrlässigkeit. Der Inhalt dieser Unterlagen kann von All for One Group SE jederzeit geändert werden. Diese Unterlagen dienen ausschließlich informativen Zwecken und dürfen in keinen Vertrag aufgenommen, für Handelszwecke weiterverwendet oder an Dritte weitergegeben werden, soweit sie nicht für eine solche Verwendung gekennzeichnet sind oder eine vorherige schriftliche Genehmigung von All for One Group SE vorliegt.